PCT/EP 0 0 / 0 2 4 8 1

# BUNDESREPUBLIK DEUTSCHLAND

EP00/2481
EJU

**PRIORITY DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)



#5
2/5/02
amr

## Bescheinigung

Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur Ableitung von Identifikationsnummern"

am 30. März 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung. Die nachgereichte Figur 5 ist am 15. Januar 2000 eingegangen.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 07 C 15/00 der Internationalen Patentklassifikation erhalten.

München, den 13. März 2000
**Deutsches Patent- und Markenamt**
**Der Präsident**
Im Auftrag

Aktenzeichen: 199 14 407.9

Nietie

A 9161
06.90
11/98

P98141

# Verfahren zur Ableitung von Identifikationsnummern

Die Erfindung betrifft ein Verfahren zur Ableitung einer Personen-Identifikations-Nummer (PIN), bestehend aus einer Anzahl N dezimaler Ziffern, zur Benutzung von Geldkarten und anderen sicherheitsbedürftigen Einrichtungen aus einer binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode.

Bei der Verwendung automatischer Geldausgabesysteme oder ähnlicher mit einer Plastikkarte zu benutzenden Einrichtungen muß sich der Benutzer häufig mittels einer nur ihm bekannten vierstelligen Nummer (PIN) authorisieren. Es gibt jedoch bei weitem nicht soviele verschiedene PINs wie Benutzer, weshalb jede PIN mehrfach existiert.

Die PINs dürfen nur dezimale Ziffern enthalten, damit sie mit numerischen Tastaturen eingegeben werden können. Ferner sollen sie nicht mit einer Null beginnen. Daraus ergibt sich bei vier Stellen ein Bereich von 9000 unterschiedlichen PINs. Die theoretisch geringstmögliche Wahrscheinlichkeit, eine PIN zu erraten, beträgt somit 1/9000.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren anzugeben, welches die Wahrscheinlichkeit möglichst gering hält, daß eine PIN erraten werden kann.

...

Der Erfindung liegt die Erkenntnis zugrunde, daß, wenn die PINs so erzeugt werden, daß sie statistisch gleichmäßig auf den zur Verfügung stehenden Zahlenbereich verteilt sind, die Wahrscheinlichkeit, eine PIN zu erraten, minimal wird. Dies wird anhand des folgenden Beispiels erläutert.

Aus persönlichen Daten des Benutzers kann mit einem geheimen Schlüssel unter Zuhilfenahme eines Verschlüsselungsalgorithmus ein Binärcode erzeugt werden. Bei Verwendung des beispielsweise zur Erzeugung von PINs für Geldkarten vorgesehenen DES- oder Triple-DES-Algorithmus' wird mit Hilfe eines bankeigenen Schlüssels aus den Daten eines Kunden ein 64-stelliger Binärcode generiert. Aus einem Abschnitt von 16 Stellen dieses Binärcodes kann die PIN beispielsweise auf folgende Weise erzeugt werden:

Es werden vier Teile zu jeweils vier Stellen dieser binären Zahl zu vier Dezimalzahlen zusammengefaßt. Die vier Ziffern der PIN ergeben sich als Rest einer Division dieser vier Dezimalzahlen durch 10 (Modulo-Funktion). Falls die erste Ziffer eine Null ist, wird sie gegen eine Eins ausgetauscht. Die daraus resultierenden PINs sind jedoch in hohem Maße ungleichmäßig über den zur Verfügung stehenden Zahlenbereich von 1 bis 9000 verteilt. Die Wahrscheinlichkeit, eine derartig erzeugte PIN zu erraten, ist gar höher als 1/150, falls sie mit einer 1 beginnt.

Verteilt man die PINs dagegen gleichmäßig über den Zahlenbereich, so ist die Auftretenshäufigkeit einer jeden PIN konstant 1/9000 und daher ist auch die Wahrscheinlichkeit minimal, daß sie erraten wird.

Eine erste Ausgestaltung der Erfindung sieht vor, daß die ersten n1 Stellen der binären Zahl (B) auf an sich bekannte Weise in eine Dezimalzahl d1 umgesetzt werden, wobei die vorgebbare natürliche Zahl n1 so gewählt wird, daß es eine

...

derartige natürliche Zahl z1 gibt, daß der Quotient $2^{n1}/(z1*9)$ nahe bei 1 liegt, und daß die erste Dezimalziffer der PIN den Wert d1 Modulo 9 erhält, daß N-1 weitere Gruppen von jeweils weiteren n2 Stellen der binären Zahl (B) auf an sich bekannte Weise in N-1 Dezimalzahlen d2 bis dN umgesetzt werden, wobei die vorgebbare Zahl n2 so gewählt wird, daß es eine derartige natürliche Zahl z2 gibt, daß der Quotient $2^{n2}/(z2*10)$ nahe bei 1 liegt, der Bedingung genügen soll: $0<=2^{n2}$ Modulo 10<3, und daß die Dezimalziffern 2 bis N der PIN die Werte di Modulo 10, i=2 bis N erhalten.

Zur Erzeugung der ersten Ziffer der PIN wird n1 so gewählt, daß $2^{n1}$ in der Nähe eines Vielfachen von 9 liegt. Der vornstehende n1-stellige Teil der binären Zahl wird als Dezimalzahl interpretiert. Es wird der ganzzahlige Rest bei einer Division durch 9 ermittelt. Dieser Rest bildet die erste Ziffer der PIN. Zur Erzeugung der Ziffern 2 und folgende der PIN werden je n2 bits abgespalten. Die Zahl n2 ist so gewählt, daß $2^{n}$ in der Nähe eines Vielfachen von 10 liegt. Die resultierende Zahl wird als Dezimalzahl interpretiert. Es wird der ganzzahlige Rest bei einer Division durch 10 ermittelt. Dieser Rest bildet die jeweilige Ziffer der PIN. Hierdurch ergibt sich zwar keine absolute Gleichverteilung. Die PIN-Ziffern sind aber umso gleichmäßiger verteilt, je größer n2 ist.

Wird beispielsweise n2=13 gewählt, so ergibt sich ein Zahlenbereich von 1 bis $2^{13}$=8192. Die Ziffern 0, 1, 2 und 3 treten in den erzeugten PINs mit einer Wahrscheinlichkeit von 820/8192 und die restlichen Ziffern mit einer Wahrscheinlichkeit von 819/8192 auf. Insbesondere wird bei dem erfindungsgemäßen Verfahren vermieden, daß die 1 in der ersten Stelle der PIN übermäßig häufig auftritt.

...

Bei einer Weiterbildung der Erfindung ist vorgesehen, daß n1 und n2<=16 vorgegeben werden.

Bei einer nächsten Weiterbildung der Erfindung ist vorgesehen, daß N=4 gewählt wird.

Es kann ferner vorgesehen sein, daß die binäre Zahl (B) die Länge L=16 aufweist, daß N=4 vorgegeben wird und daß n1=n2=4 vorgegeben werden.

Eine andere Ausgestaltung der Erfindung besteht darin, daß die binäre Zahl (B) die Länge L=3*n3 aufweist, daß n3 Gruppen von jeweils drei Stellen der binären Zahl (B) auf an sich bekannte Weise zur Bildung der Ziffern der PIN in n3 Dezimalziffern umgesetzt werden, wobei n3 eine natürliche Zahl ist. Bei dieser Variante werden insgesamt 12 bit des kundenspezifischen Binärcodes zur Erzeugung der PIN benutzt. Je 3 bit dieser Binärzahl werden als Dezimalziffer zwischen 1 und 8 interpretiert. Die damit erzeugten PINs sind absolut gleichmäßig verteilt.

Eine weitere Möglichkeit, innerhalb des jeweiligen Zahlenbereiches absolut gleichverteilte PINs zu erzeugen, besteht darin, daß die binäre Zahl zur Bildung der PIN in an sich bekannter Weise komplett in eine Dezimalzahl umgesetzt wird und daß zu der sich ergebenden Dezimalzahl erforderlichenfalls ein derartiger Korrekturwert hinzuaddiert wird, daß die erste Ziffer der Dezimalzahl ungleich Null wird, wobei die Ziffern des Ergebnisses die Ziffern der PIN bilden.

Es kann dazu vorgesehen sein, daß die Länge L der binären Zahl 13 beträgt, daß die erzeugte Dezimalzahl vier Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 999 und kleiner als 1807 hinzuaddiert wird, oder daß die Länge L der binären Zahl 16 beträgt, daß die

...

erzeugte Dezimalzahl fünf Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 9999 und kleiner als 34465 hinzuaddiert wird.

Im ersten Fall (L=13) kann ferner vorgesehen sein, daß die Menge der Zahlen 0 bis 8191 in n5 Teilmengen M1,...,Mn5 aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge Mi ist, ein fest vorgegebener Wert di hinzuaddiert wird, wobei gilt 999<d1<d2<...<dn5<1809 und wobei n5 eine natürliche Zahl ist.

Im zweiten Fall (L=16) kann ferner vorgesehen sein, daß die Menge der Zahlen 0 bis 65535 in n5 Teilmengen M1,...,Mn5 aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge Mi ist, ein fest vorgegebener Wert di hinzuaddiert wird, wobei gilt 9999<d1<d2<...<dn5<34465 und wobei n5 eine natürliche Zahl ist.

Eine weitere vorgeschlagene Ausgestaltung der Erfindung besteht darin, daß zur Erstellung der ersten Ziffer der PIN folgende Schritte ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 36 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 36 möglichen mathematischen Abbildungen hexadezimaler Ziffern in die Ziffern 1 bis 9 in eine Ziffer aus den Ziffern von 1 bis 9 umgesetzt,
- die bis zu 36 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer ungleich Null verknüpft, welche die erste Ziffer der PIN darstellt,

und daß folgende Schritte jeweils für die zweite und jede folgende Ziffer der zu erstellenden PIN ausgeführt werden:

...

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 210 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 210 möglichen mathematischen Abbildungen hexadezimaler Ziffern in dezimale Ziffern in eine dezimale Ziffer umgesetzt,
- die bis zu 210 dezimalen Ziffer der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer verknüpft, welche die jeweilige Ziffer der PIN darstellt.

Dazu kann vorgesehen sein, daß die erste Ziffer der PIN gebildet wird, indem die bis zu 36 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 verknüpft werden und daß die zweite und die folgenden Ziffern der PIN gebildet werden, indem die jeweils bis zu 210 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 10 verknüpft werden.

Bei dieser Ausgestaltung des erfindungsgemäßen Verfahrens wird aus N Gruppen von jeweils 4 bit Länge je eine Hexadezimalzahl gebildet. Diese soll nun in eine Dezimalziffer umgesetzt werden. Für diese Umsetzung stehen insgesamt (10 über 6) = (10 über 4) = 210 unterschiedliche Abbildungen der hexadezimalen Ziffern in die Menge der dezimalen Ziffern zur Verfügung. Eine mögliche Abbildung ist die Bildung des Rests bei der Division durch 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Nach dieser Abbildung treten die Ziffern 0 bis 5 jeweils mit der Häufigkeit von 1/8 und die Ziffern von 6 bis 9 mit der Häufigkeit 1/16 auf. Um nun Ziffern zu erhalten, deren Auftretenswahrscheinlichkeit nicht oder unmerklich von 1/10

...

abweicht, wird vorgeschlagen, die 210 Hexadezimalziffern, die beispielsweise durch 14-maliges Anwenden des o.g. DES-Algorithmus auf die 64-stellige binäre Ausgangszahl erzeugt wurden (daher Pseudo-Zufallszahl, da die erzeugte Zahl mitnichten zufällig entstanden ist), mit je einer anderen der 210 möglichen Abbildungen in eine Dezimalziffer umzusetzen und anschließend alle 210 Dezimalziffern mit einer Gruppenoperation einer mathematischen Gruppe mit zehn Elementen zu einer einzigen Ziffer zu verknüpfen. Die Auftretenswahrscheinlichkeit jeder so erzeugten dezimalen Ziffer liegt nahe bei 1/10.

Es ist bei einer nächsten Weiterbildung der Erfindung vorgesehen, daß die additive Gruppe der ganzen Zahlen Modulo 10 zur Verknüpfung der bis zu 210 Ziffern verwendet wird. Es werden dabei jeweils 210 Dezimalziffern zu einer einzigen Ziffer verknüpft, indem man alle Ziffern addiert und den Rest einer Division der Summe durch 10 als Ergebnis nimmt. Die dabei auftretenden zehn möglichen Ergebnisse sind die Elemente der additiven Gruppe $Z_{10,+}$.

Bei einer anderen Weiterbildung der Erfindung ist vorgesehen sein, daß die multiplikative Gruppe der ganzen Zahlen Modulo 11 zur Verknüpfung der bis zu 210 Ziffern verwendet wird. Diese Gruppe $Z^*_{11}$ weist ebenfalls zehn Elemente auf und eignet sich daher zur Verknüpfung der Zahlen zu einer Dezimalziffer. In $Z^*_{11}$ rechnet man, indem man zwei Elemente multipliziert und das Ergebnis durch 11 dividiert. Der dabei bleibende Rest bildet das Ergebnis der Operation. Die Null ist aus der Gruppe ausgenommen. Die in den Ziffern auftretende 0 indiziert das Element Nr. 10 der Gruppe $Z^*_{11}$.

Eine andere Weiterbildung der Erfindung sieht vor, daß die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks (Diedergruppe) zur Verknüpfung der bis zu 210 Ziffern verwendet wird, wobei jeder der zehn Symmetrieabbildungen

...

dieser Gruppe eine andere dezimale Ziffer zugeordnet wird. Dazu kann ferner vorgesehen sein, daß der Identitätsabbildung die Ziffer 0, den vier Drehungen um den Mittelpunkt des Fünfecks die Ziffern 1 bis 4 und den fünf Spiegelungen um die fünf Symmetrieachsen des Fünfecks die Ziffern 5 bis 9 zugeordnet werden. Führt man zwei Symmetrieabbildungen hintereinander aus, so entsteht wieder eine Symmetrieabbildung. Es läßt sich mit diesen Zuordnungen die folgende Multiplikationstabelle aufstellen:

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 1 | 2 | 3 | 4 | 0 | 6 | 7 | 8 | 9 | 5 |
| 2 | 2 | 3 | 4 | 0 | 1 | 7 | 8 | 9 | 5 | 6 |
| 3 | 3 | 4 | 0 | 1 | 2 | 8 | 9 | 5 | 6 | 7 |
| 4 | 4 | 0 | 1 | 2 | 3 | 9 | 5 | 6 | 7 | 8 |
| 5 | 5 | 9 | 8 | 7 | 6 | 0 | 4 | 3 | 2 | 1 |
| 6 | 6 | 5 | 9 | 8 | 7 | 1 | 0 | 4 | 3 | 2 |
| 7 | 7 | 6 | 5 | 9 | 8 | 2 | 1 | 0 | 4 | 3 |
| 8 | 8 | 7 | 6 | 5 | 9 | 3 | 2 | 1 | 0 | 4 |
| 9 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0. |

Die 210 Ziffern werden mit Hilfe dieser Tabelle zu einer einzigen Ziffer verknüpft, indem sukzessiv mit dem Ergebnis der letzten Operation als Zeilenindikator und mit der nächsten Ziffer als Spaltenindikator das nächste Ergebnis in der Tabelle abgelesen wird, bis alle Ziffern berücksichtigt wurden. Das letze Ergebnis bildet die gesuchte Ziffer der PIN.

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 ein Diagramm zur Erzeugung eines kundenspezifischen Binärcodes,

Fig. 2 ein Diagramm zur Erzeugung einer PIN durch Umwandlung in eine Dezimalzahl,

...

Fig. 3 ein Diagramm zur Erzeugung einer PIN durch ziffernweise Umwandlung in Dezimalzahlen,

Fig. 4 ein Diagramm zur Erzeugung einer PIN durch ziffernweise Umsetzung mit Modulbildung und

Fig. 5 ein Diagramm zur Erzeugung einer PIN durch Reduktion von Hexadezimalzahlen mit Hilfe mathematischer Gruppen.

Gleiche Teile sind in den Figuren mit gleichen Bezugszeichen versehen.

Fig. 1 zeigt ein Ablaufdiagramm zur Umsetzung von persönlichen Daten Dc eines Kunden mit Hilfe eines geheimen Schlüssels K in eine binäre Zahl B von L bit Länge. Die binäre Zahl B ist Teil des 64 bit langen Verschlüsselungsergebnisses, welches aus den Kundendaten Dc mit dem DES-Algorithmus erzeugt wurde.

Sei die Länge der binären Zahl B gleich 13 und sei die Anzahl der zu erzeugenden Ziffern der PIN gleich 4, so kann die PIN, wie in Fig. 2 gezeigt wird, dadurch erzeugt werden, daß die binäre Zahl B als Dezimalzahl D interpretiert und dazu eine Konstante C addiert wird. Die Konstante ist so zu wählen, daß die PIN keine führenden Nullen aufweist. Auf diese Weise können 8192 unterschiedliche PINs erzeugt werden, die über den jeweiligen Zahlenbereich absolut gleichmäßig verteilt sind.

Fig. 3 zeigt, wie eine binäre Zahl der Länge 13 in eine PIN umgewandelt werden kann, indem man je Ziffer der zu erzeugenden PIN eine Anzahl bits der binären Zahl in eine Dezimalzahl umwandelt und zu der sich daraus ergebenden Zahl D eine Konstante C addiert, um führende Nullen der PIN zu vermeiden. Auf diese Weise können 7777 unterschiedliche PINs

...

erzeugt werden, die über dem jeweiligen Zahlenbereich absolut gleichmäßig verteilt sind.

Eine weitere Möglichkeit zur Erzeugung annähernd gleich verteilter PINs aus einer binären Zahl B ist in Fig. 4 dargestellt. Die binäre Zahl B habe 52 Stellen. Zur Erzeugung der vierstelligen PIN wird die binäre Zahl B in vier Teile unterteilt, die im Beispiel die gleiche Länge haben. Jedes dieser Teile wird als Dezimalzahl interpretiert. Die erste Ziffer der PIN ergibt sich als Rest einer Division der ersten Dezimalzahl durch 9. Die folgenden Ziffern der PIN ergeben sich jeweils als Rest der Division der folgenden Dezimalzahlen durch 10. Auf diese Weise können 9000 unterschiedliche PINs erzeugt werden, die absolut gleichmäßig verteilt sind.

Aus den persönlichen Daten Dc eines Kunden werden, wie in Fig. 5 gezeigt, mit Hilfe eines geheimen Schlüssels und eines Zufallszahlen-Generators eine Folge von 210 Hexadezimalziffern erzeugt, indem beispielsweise ein Verschlüsselungsergebnis des DES-Algorithmus aus Fig. 1 wiederum mit dem Algorithmus verschlüsselt wird und so fort. Die daraus resultierenden 14 64-stelligen Binärcodes werden in 14 Hexadezimalzahlen Hi mit je 16 Stellen gewandelt. Aneinandergehängt gibt das 224 Hexadezimalziffern, wovon 210 in die Erzeugung der PIN eingehen.

Es gibt 210 unterschiedliche Möglichkeiten fi, die Menge der 16 Hexadezimalziffern in die Menge der 10 Dezimalziffern abzubilden. Jede der 210 Hexadezimalziffern wird daher mit einer anderen dieser Abbildungen in eine Dezimalziffer di umgesetzt. Um aus den 210 Dezimalziffern eine Ziffer Zi einer PIN zu erzeugen, werden diese mit Hilfe der Gruppenoperation F einer beliebigen zehnelementigen mathematischen Gruppe nacheinander verknüpft; das letzte Ergebnis ist die gesuchte Ziffer. Die vorher ungleichmäßige

...

statistische Verteilung der 210 Dezimalziffern wird damit vergleichmäßigt. Der gesamte Vorgang wird für jede der Stellen Z2 bis Z4 der PIN erneut durchgeführt.

Für die erste Ziffer der PIN werden analog 36 Hexadezimalziffern erzeugt, die mit je einer anderen der 36 möglichen Abbildungen der Hexadezimalziffern in die Menge der Ziffern 1 bis 9 in eine Ziffer zwischen 1 und 9 abgebildet werden. Die 36 Dezimalziffern werden mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 zu der ersten Ziffer der PIN verknüpft. Es lassen sich damit 9000 unterschiedliche PINs erzeugen, die annähernd gleichmäßig verteilt sind. Bei der Erzeugung von $10^5$ PINs betrugen die maximalen Ungleichmäßigkeiten etwa 1,5 Prozent, was die Wahrscheinlichkeit, daß eine PIN zufällig erraten wird, nicht nennenswert gegenüber dem theoretischen Minimalwert erhöht. Das Verfahren arbeitet damit sehr zuverlässig.

Zur Anwendung in diesem Verfahren eignen sich grundsätzlich alle mathematischen Gruppen, die zehn Elemente aufweisen. Bekannte Vertreter sind die additive Gruppe der ganzen Zahlen Modulo 10, $Z_{10,+}$, die multiplikative Gruppe der ganzen Zahlen Modulo 11, $Z^*_{11}$, sowie die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks D5, die sogenannte Diedergruppe. Im letzten Falle wird den einzelnen Elementen der Gruppe je eine Dezimalziffer zugeordnet, mit der sich rechnen läßt.

...

Ansprüche

1. Verfahren zur Ableitung einer Personen-Identifikations-Nummer (PIN), bestehend aus einer Anzahl N dezimaler Ziffern, zur Benutzung von Geldkarten und anderen sicherheitsbedürftigen Einrichtungen aus einer binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode, dadurch gekennzeichnet, daß die PINs so erzeugt werden, daß sie statistisch gleichmäßig auf den zur Verfügung stehenden Zahlenbereich verteilt sind.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die ersten n1 Stellen der binären Zahl (B) auf an sich bekannte Weise in eine Dezimalzahl d1 umgesetzt werden, wobei die vorgebbare natürliche Zahl n1 so gewählt wird, daß es eine derartige natürliche Zahl Z1 gibt, daß der Quotient $2^{n1}/(Z1*9)$ nahe bei 1 liegt, und daß die erste Dezimalziffer der PIN den Wert d1 Modulo 9 erhält, daß N-1 weitere Gruppen von jeweils weiteren n2 Stellen der binären Zahl (B) auf an sich bekannte Weise in N-1 Dezimalzahlen d2 bis dN umgesetzt werden, wobei die vorgebbare Zahl n2 so gewählt wird, daß es eine derartige natürliche Zahl Z2 gibt, daß der Quotient $2^{n2}/(Z2*10)$ nahe bei 1 liegt, der Bedingung genügen soll: $0<=2^{n2}$ Modulo $10<3$, und daß die Dezimalziffern 2 bis N der PIN die Werte di Modulo 10, i=2 bis N erhalten.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß n1 und $n2<=16$ vorgegeben werden.

...

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß N=4 gewählt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die binäre Zahl (B) die Länge L=16 aufweist, daß N=4 vorgegeben wird und daß n1=n2=4 vorgegeben werden.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die binäre Zahl (B) die Länge L=3*n3 aufweist, daß n3 Gruppen von jeweils drei Stellen der binären Zahl (B) auf an sich bekannte Weise zur Bildung der n3 Ziffern der PIN in n3 Dezimalziffern umgesetzt werden, wobei n3 eine natürliche Zahl ist.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die binäre Zahl (B) zur Bildung der PIN in an sich bekannter Weise komplett in eine Dezimalzahl umgesetzt wird und daß zu der sich ergebenden Dezimalzahl erforderlichenfalls ein derartiger Korrekturwert hinzuaddiert wird, daß die erste Ziffer der Dezimalzahl ungleich Null wird, wobei die Ziffern des Ergebnisses die Ziffern der PIN bilden.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Länge L der binären Zahl (B) 13 beträgt, daß die erzeugte Dezimalzahl vier Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 999 und kleiner als 1807 hinzuaddiert wird.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Menge der Zahlen 0 bis 8191 in n5 Teilmengen M1,...,Mn5 aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge Mi ist, ein fest vorgegebener Wert di hinzuaddiert wird, wobei gilt 999<d1<d2<...<dn5<1809 und wobei n5 eine natürliche Zahl ist.

...

10. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Länge L der binären Zahl (B) 16 beträgt, daß die erzeugte Dezimalzahl fünf Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 9999 und kleiner als 34465 hinzuaddiert wird.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß die Menge der Zahlen 0 bis 65535 in n5 Teilmengen M1,...,Mn5 aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge Mi ist, ein fest vorgegebener Wert di hinzuaddiert wird, wobei gilt 9999<d1<d2<...<dn5<34465 und wobei n5 eine natürliche Zahl ist.

12. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Erstellung der ersten Ziffer der PIN folgende Schritte ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 36 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 36 möglichen mathematischen Abbildungen hexadezimaler Ziffern in die Ziffern 1 bis 9 in eine Ziffer aus den Ziffern von 1 bis 9 umgesetzt,
- die bis zu 36 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer ungleich Null verknüpft, welche die erste Ziffer der PIN darstellt,

und daß folgende Schritte jeweils für die zweite und jede folgende Ziffer der zu erstellenden PIN ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 210 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 210 möglichen mathematischen

...

Abbildungen hexadezimaler Ziffern in dezimale Ziffern in eine dezimale Ziffer umgesetzt,

- die bis zu 210 dezimalen Ziffer der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer verknüpft, welche die jeweilige Ziffer der PIN darstellt.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß die erste Ziffer der PIN gebildet wird, indem die bis zu 36 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 verknüpft werden und daß die zweite und die folgenden Ziffern der PIN gebildet werden, indem die jeweils bis zu 210 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 10 verknüpft werden.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die additive Gruppe der ganzen Zahlen Modulo 10 zur Verknüpfung der bis zu 210 Ziffern verwendet wird.

15. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die multiplikative Gruppe der ganzen Zahlen Modulo 11 zur Verknüpfung der bis zu 210 Ziffern verwendet wird.

16. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks (Diedergruppe) zur Verknüpfung der bis zu 210 Ziffern verwendet wird, wobei jeder der zehn Symmetrieabbildungen dieser Gruppe eine andere dezimale Ziffer zugeordnet wird.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, daß der Identitätsabbildung die Ziffer 0, den vier Drehungen um den Mittelpunkt des Fünfecks die Ziffern 1 bis 4 und den

...

fünf Spiegelungen um die fünf Symmetrieachsen des Fünfecks die Ziffern 5 bis 9 zugeordnet werden.

...

Zusammenfassung

Bei einem Verfahren zur Ableitung einer Personen-Identifikations-Nummer (PIN), bestehend aus einer Anzahl N dezimaler Ziffern, zur Benutzung von Geldkarten und anderen sicherheitsbedürftigen Einrichtungen aus einer binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode, werden die PINs so erzeugt, daß sie statistisch gleichmäßig auf den zur Verfügung stehenden Zahlenbereich verteilt sind.

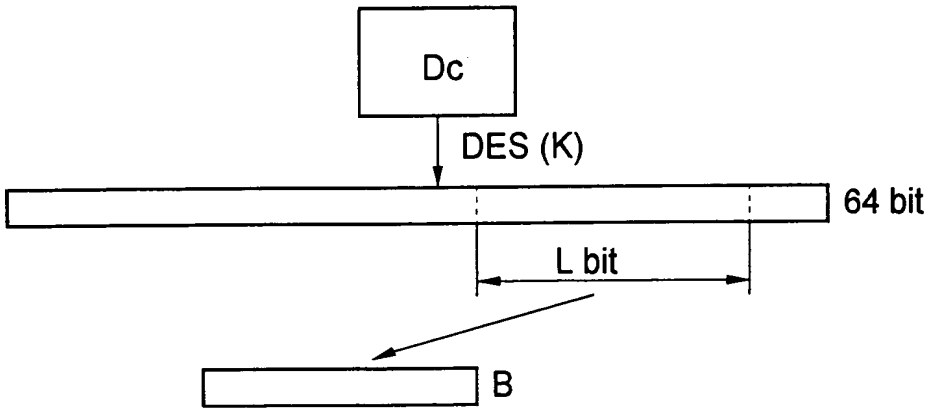


Fig.1

L = 13,
N = 4,
PINmax-PINmin=8192

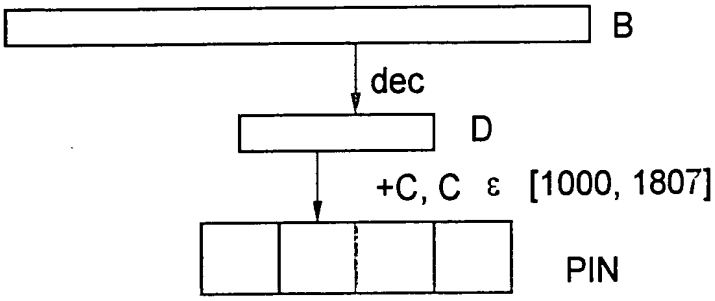


Fig.2

L = 12,
N = 4,
PINmax-PINmin=7777

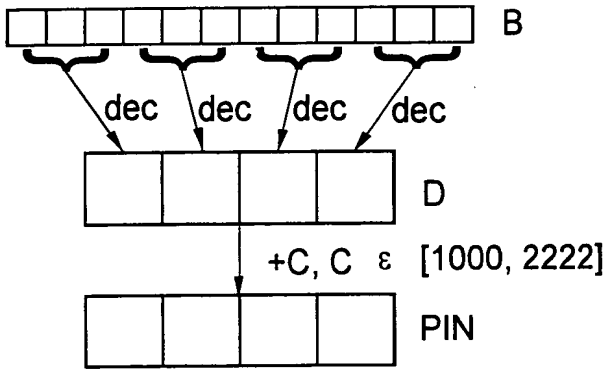


Fig.3

L = 52,
N = 4,
PINmax-PINmin=9000

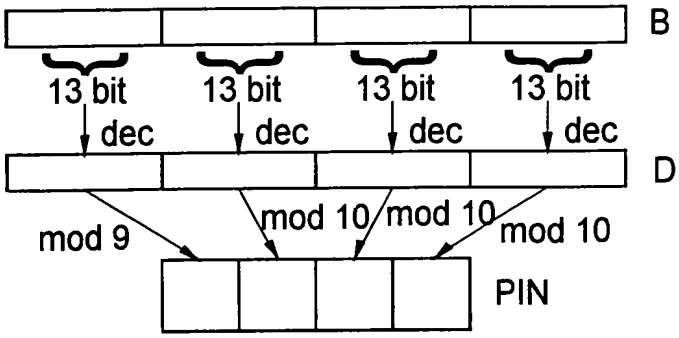


Fig.4

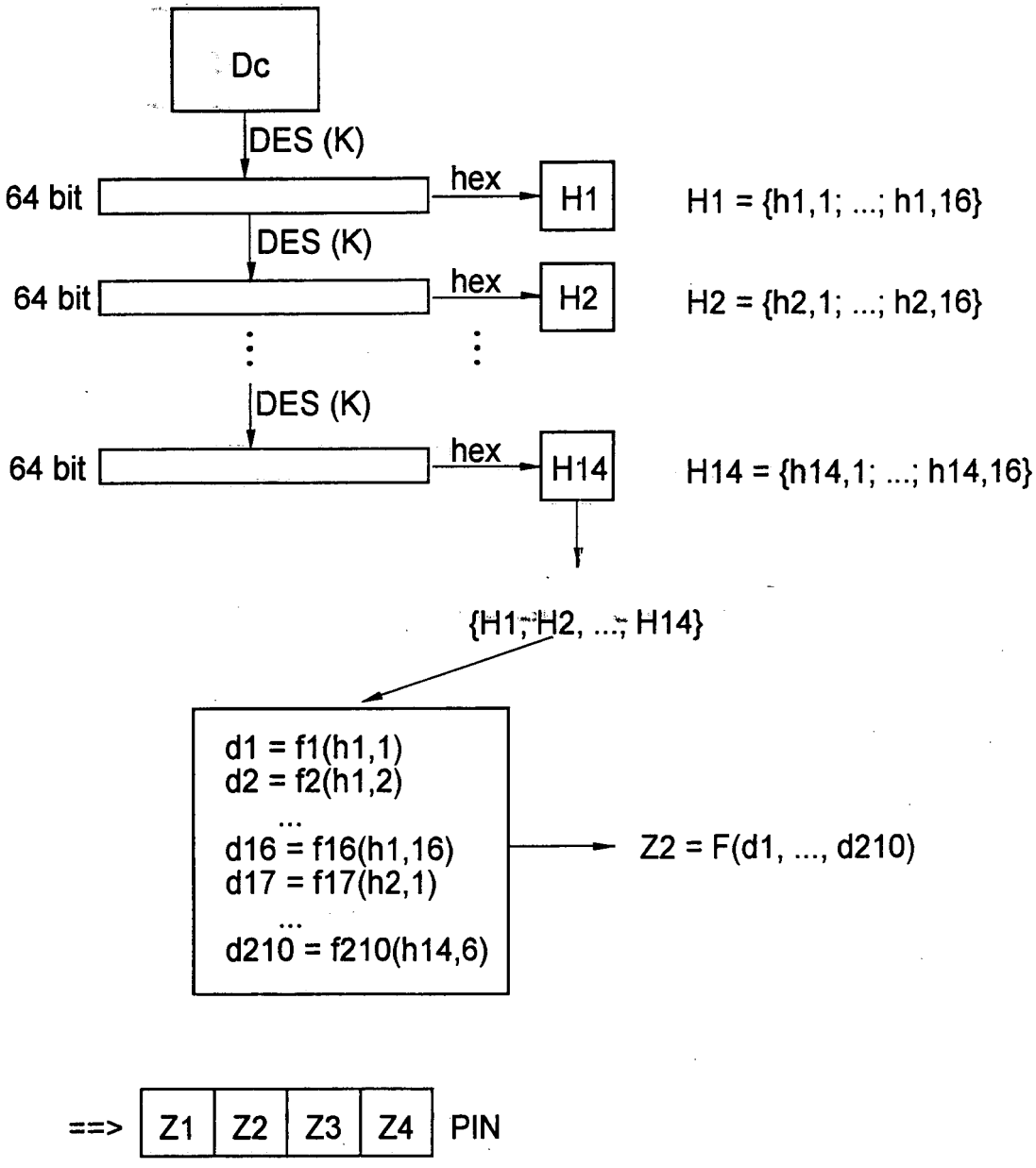
Dc
DES (K)
64 bit
hex
H1
H1 = {h1,1; ...; h1,16}
DES (K)
64 bit
hex
H2
H2 = {h2,1; ...; h2,16}
DES (K)
64 bit
hex
H14
H14 = {h14,1; ...; h14,16}
{H1; H2, ...; H14}
d1 = f1(h1,1)
d2 = f2(h1,2)
...
d16 = f16(h1,16)
d17 = f17(h2,1)
...
d210 = f210(h14,6)
Z2 = F(d1, ..., d210)
==>
Z1
Z2
Z3
Z4
PIN

Fig.5